



SMCBR14VPN/SMCBR18VPN
Barricade™
VPN 4/8-port Broadband Router

USER GUIDE

Copyright

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

The products and programs described in this User Guide are licensed products of SMC. This User Guide contains proprietary information protected by copyright, and this User Guide and all accompanying hardware and documentation are copyrighted.

SMC does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

Information in this User Guide is subject to change without notice and does not represent a commitment on the part of SMC. SMC assumes no responsibility for any inaccuracies that may be contained in this User Guide.

SMC makes no commitment to update or keep current the information in this User Guide, and reserves the right to make changes to this User Guide and/or product without notice.

No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of SMC.

Copyright © 2004 by
SMC Networks, Inc.
38 Tesla
Irvine, California 92618
All rights reserved.

Trademarks

SMC® is a registered trademark; and EZ-Stream, EZ Connect, Barricade and EZ Hub are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Compliances

FCC - Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: To assure continued compliance, (for example - use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION STATEMENT:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 5 centimeters between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Note: In order to maintain compliance with the limits of a Class B digital device, SMC requires that you use a quality interface cable when connecting to this device. Changes or modifications not expressly approved by SMC could void the user's authority to operate this equipment.

Attach unshielded twisted-pair cable (UTP) to the RJ-45 port and shielded USB cable to the USB port.

EC Conformance Declaration - Class B

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II
Calle Fructuos Gelabert 6-8, 2o, 4a
08970 - Sant Joan Despi
Barcelona, Spain

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B, and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the member states relation to electromagnetic compatibility.

Important Safety Notices

- Unplug this product from the AC power before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a dry cloth for cleaning.
- Route the power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords at plugs, convenience receptacles, and the point where they exit from the product.
- Situate the product away from heat sources such as radiators, heat registers, stoves, and other products that produce heat.
- To prevent fire or shock hazard, do not expose this unit to rain or moisture. Do not allow water or any foreign objects to enter the interior. This may cause a fire or electric shock. In the event that water or other foreign objects get into the product, immediately unplug the AC adapter from the electrical outlet and contact Customer Service for inspection and/or repair/replacement options.
- Do not take apart the equipment. This may cause fire, electric shock or other injuries.
- Do not overload wall outlets and extension cords as this can result in a fire or electric shock.
- This product is for use with the AC adapter that comes with it. Use with any other AC power is strongly discouraged as it may cause fire, electric shock, or damage to the equipment.

1 SYSTEM REQUIREMENTS	1
2 EQUIPMENT CHECKLIST	1
3 FUNCTIONS AND FEATURES	2
4 PANEL LAYOUT	3
5 HARDWARE INSTALLATION	4
6 NETWORK SETTINGS AND SOFTWARE INSTALLATION	4
6.1 Installing TCP/IP	5
6.2 Setting up TCP/IP	5
6.3 Obtaining an IP Address	6
6.4 Configuring a Macintosh Computer	7
6.5 Verifying Your TCP/IP Connection	7
7 CONFIGURING YOUR BROADBAND VPN ROUTER	8
7.1 Browser Configuration	8
7.2 Web Management	8
7.3 Setup Wizard	9
7.4 Advanced Setup - SYSTEM	16
7.5 Advanced Setup - WAN	19
7.6 Advanced Setup - LAN	24
7.7 Advanced Setup - NAT	26
7.7.1 Virtual Server	26
7.7.2 Special Applications	27
7.7.3 Virtual Computer	28
7.8 Advanced Setup - FIREWALL	28
7.8.1 Network Filters	28
7.8.2 URL Blocking	29
7.8.3 MAC Filter	30
7.8.4 Schedule Rule	31
7.8.5 Advanced	32
7.8.6 DMZ	33

7.9 Advanced Setup - VPN	33
7.9.1 IPSec Tunnel	33
7.9.2 IKE Proposal	35
7.9.3 IPSec Proposal	36
7.9.4 Dynamic VPN	38
7.9.5 PPTP/L2TP Server	39
7.10 Advanced Setup - SNMP	40
7.11 Advanced Setup - ROUTING	41
7.12 Advanced Setup - MISCELLANEOUS	42
7.13 Advanced Setup - DISPLAY STATUS	43
7.14 DDNS (Dynamic DNS)	43
7.15 UPnP (Universal Plug-and-Play)	44
7.16 Tools	44
7.17 Status	45
8 IPSEC SETTINGS GUIDE (FOR REFERENCE/EXAMPLE ONLY)	47
8.1 Tunnel between two SMCBR14VPN	47
8.1.1 Settings for Router 1	47
8.1.2 Settings for router 2	49
8.1.3 Common Settings for both routers	52
8.2 Tunnel between a SMCBR14VPN and standalone client.	53
8.3 PPTP/ L2TP configuration example	54
9 TROUBLESHOOTING	56
9.1 Questions and Answers	59
10 TECHNICAL SPECIFICATIONS	60
11 TERMINOLOGY	62

1 | System Requirements

- Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem, cable modem, Dial-Up modem, or ISDN modem
- A PC using a fixed IP address or dynamic IP address assigned via DHCP, as well as a Gateway server address and DNS server address from your service provider
- A computer equipped with a 10 Mbps, 100 Mbps, or 10/100 Mbps Fast Ethernet card, or a USB-to-Ethernet converter
- TCP/IP network protocol installed on each PC that needs to access the internet
- A Java-enabled web browser, such as Microsoft Internet Explorer 5.0 or above, or Netscape Communicator 4.0 or above installed on one PC at your site for configuring the router.

2 | Equipment Checklist

After unpacking the Barricade™ VPN Cable/DSL Broadband Router, check the contents of the box to be sure you have received the following components:

- 1 Barricade™ VPN Cable/DSL Broadband Router
- 1 EZ Installation Wizard and Documentation CD
- 1 Ethernet (CAT5-UTP/Straight-Through) Cable
- 1 Power Adapter
- 1 Quick Installation Guide

Immediately inform your dealer in the event of any incorrect, missing or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

Please register this product and upgrade the product warranty at SMC's Web site:

<http://www.smc.com>

3 | Functions and Features

Broadband Modem and NAT Router	Connects multiple computers to a broadband (cable or DSL) modem, and/or Ethernet router to access the Internet.
10/100 Mbps Ethernet Interface	Provides a 10/100 Base-TX interface to connect to a DSL or cable modem for broadband Internet access.
Auto-sensing Ethernet Switch	Equipped with a 4/8-port auto-sensing Ethernet switch.
VPN Supported	Supports multiple IPsec sessions and has built-in PPTP and L2TP VPN servers.
Firewall	All unwanted packets from outside sources are blocked to protect your intranet.
DHCP Server Supported	All networked computers can retrieve TCP/IP settings automatically from this device.
Web-based Configuration	Configurable by any networked computer's Web browser using Netscape or Internet Explorer.
Network Filter Supported	The Packet Filter lets you control access to a network by analyzing the incoming and outgoing packets; this lets you either letting them pass or halt based on the IP address or the source and destination.
Universal Plug and Play (UPnP) Supported	Enables devices such as PCs, routers and printers to be plugged into a network and ensure automatic recognition.
Virtual Server Supported	Lets you make your Website, FTP site, and other services on your LAN accessible to Internet users.
User Defined Application Sensing Tunnel	Lets you define the attributes to support special applications that require multiple connections like Internet gaming, video conferencing, Internet telephony, and so on. This device can sense the application type and opens a multi-port tunnel for it.
DMZ Host Supported	Enables a computer to be fully accessible to the Internet. This function is used when the special application sensing tunnel feature is insufficient to allow an application to function correctly.
SNMP Supported	SNMP (Simple Network Management Protocol) is a protocol that lets users remotely manage a computer network by polling and setting terminal values, and monitoring network events.
System Time Supported	Lets you synchronize system time with the network time server.
Virtual Computers Supported	The virtual computer lets you use the original NAT feature, which lets you setup the one-to-one mapping of multiple global and local IP addresses.
URL Blocking Supported	Lets you block hundreds of Website connections by simply entering a keyword.
Schedule Rule	Lets you set a time schedule for different services.
Routing Table Supported	Allows you to determine which physical interface address to use for outgoing IP data grams. If you have more than one router and subnet, enable the routing table to allow packets to find the proper routing path and the different subnets to communicate with each other.

4 | Panel Layout

The following figure shows the front panel layout, which is followed by a table describing in detail the status and function of each LED.

SMCBR14VPN Front Panel



SMCBR18VPN Front Panel



LED	Function	Color	Status	Description
Power	Power indicator	Green	Steady	Power is being applied to this device
M1	System status indicator	Orange	Blinking	M1 is flashing once every second to indicate that the system has power
WAN	Wan port activity	Green	Steady	The WAN port is connected
			Blinking	The WAN port is sending or receiving data
Link/Act. 1-4/8	Link status	Green	Steady	An active station is connected to the LAN port
			Blinking	The corresponding LAN port is sending or receiving data
Speed 10/100	Data rate	Green	Steady	Data is transmitted at 100 Mbps

SMCBR14VPN Rear Panel: 4 LAN, 1 WAN, and 1 COM port



SMCBR18VPN Front Panel: 8 LAN, 1 WAN, and 1 COM port



Port Type	Description
5 VDC	Receptor for power adapter: 5 VDC, 2 A (minimum)
WAN	This is the connection for the Ethernet cable to the Ethernet port on the cable or DSL modem
Port 1-4/8	These are the connections for Ethernet cables to your Ethernet enabled computers
COM	Serial port (connection for an analog modem or console cable)

5 | Hardware Installation

The router can be placed anywhere in your office or home. No special wiring or cooling requirements are necessary. However, you should comply with the following guidelines:

- Place your router on a flat, horizontal surface
 - Be sure to place your router away from any heating devices
 - Avoid dusty and/or humid areas
- 1) **Setup LAN Connection:** Connect an Ethernet cable from your computer's Ethernet port to one of the LAN ports of the router.
 - 2) **Step WAN Connection:** Insert one end of the Ethernet cable into the WAN port on the back panel of your router, and the other end to the cable/DSL modem. You may connect an analog modem (optional) to function as a backup connection.
 - 3) **Power Up:** The router automatically enters the self-testing phase once the power cord is plugged into a wall outlet. When in self-testing phase, the M1 indicator LED illuminates for about five seconds to indicate proper connection. The M1 LED flashes twice as soon as the self-testing phase is completed. After the completion of the self-testing phase, the M1 LED should flash once per second to indicate that the router is functioning properly.

6 | Network Settings and Software Installation

Default Settings	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Administrator Password	smcadmin
User Password	password

You must first verify that the TCP/IP communication protocol is properly installed and the computer is configured to get its IP address via the DHCP Server that is built-into this router. If you have not previously installed TCP/IP protocols on your client PCs, refer to the following section.

6.1 | Installing TCP/IP

Windows 95/98/Me

1. Click Start/Settings/Control Panel.
2. Double-click the Network icon and select the Configuration tab in the Network window.
3. Click the Add button.
4. Double-click Protocol.
5. Select Microsoft in the manufacturers list. Select TCP/IP in the Network Protocols list. Click the OK button to return to the Network window.
6. The TCP/IP protocol will be listed in the Network window.
7. Click OK. The operating system may prompt you to restart your system. Click Yes and the computer will shut down and restart.

Windows 2000/XP

1. Click the Start button and choose Settings, then click the Network and Dial-up Connections icon.
2. Double-click the Local Area Connection icon, and click the Properties button on the General tab.
3. Click the install button.
4. Double-click Protocol.
5. Choose Internet Protocol (TCP/IP). Click the OK button to return to the Network window.
6. The TCP/IP protocol will be listed in the Network window. Click OK to complete the installation procedure.

6.2 | Setting up TCP/IP

Windows 95/98/Me

You may find that the instructions here do not exactly match your version of Windows. This is because these steps and screenshots were created in Windows 98. Windows 95 and Windows Millennium Edition are very similar, but not identical, to Windows 98.

1. From the Windows desktop, click Start/Settings/Control Panel.
2. In the Control Panel, locate and double-click the Network icon.
3. On the Network window Configuration tab, double-click the TCP/IP entry for your network card.
4. Click the IP Address tab.
5. Click the "Obtain an IP address" option.
6. Next click on the Gateway tab and verify the Gateway field is blank. If there are IP addresses listed in the Gateway section, highlight each one and click Remove until the section is empty.
7. Click the OK button to close the TCP/IP Properties window.
8. On the Network Properties Window, click the OK button to save these new settings. Note: Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM

into your CDROM drive and check the correct file location, e.g., D:\win98, D:\win9x. (if D is the letter of your CD-ROM drive).

9. Windows may prompt you to restart the PC. If so, click the Yes button. If Windows does not prompt you to restart your computer, do so to insure your settings.

Windows NT

1. From the Windows desktop click Start/Settings/Control Panel.
2. Double-click the Network icon.
3. Click on the Protocols tab.
4. Double-click TCP/IP Protocol.
5. Click on the IP Address tab.
6. In the Adapter drop-down list, be sure your Ethernet adapter is selected.
7. Click on "Obtain an IP address from a DHCP server."
8. Click OK to close the window.
9. Windows may copy files and will then prompt you to restart your system. Click Yes and your computer will shut down and restart.

Windows 2000/XP

1. Access your Network settings by clicking Start, then choose Settings and then select Control Panel.
2. In the Control Panel, locate and double-click the Network and Dial-up Connections icon.
3. Locate and double-click the Local Area Connection icon for the Ethernet adapter that is connected to the Router. When the Status dialog box window opens, click the Properties button.
4. In the Local Area Connection Properties box, verify the box next to Internet Protocol (TCP/IP) is checked. Then highlight the Internet Protocol (TCP/IP), and click the Properties button.
5. Select "Obtain an IP address automatically" to configure your computer for DHCP. Click the OK button to save this change and close the Properties window.
6. Click the OK button again to save these new changes.
7. Reboot your PC.

6.3 | Obtaining an IP Address

Windows 95/98/Me

1. Click Start/Run.
2. Type WINIPCFG and click OK.
3. From the drop-down menu, select your network card. Click Release and then Renew. Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168. 2.1. These values confirm that the Router is functioning. Click OK to close the IP Configuration window.

Windows 2000/XP

1. On the Windows desktop, click Start/Programs/Command Prompt.
2. In the Command Prompt window, type IPCONFIG /RELEASE and press the <ENTER> key.
3. Type IPCONFIG /RENEW and press the <ENTER> key. Verify that your IP Address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.254. These values confirm that the Router is functioning
4. Type EXIT and press <ENTER> to close the Command Prompt window.

6.4 | Configuring a Macintosh Computer

You may find that the instructions here do not exactly match your screen. This is because these steps and screen shots were created using Mac OS 10.2. Mac OS 7.x and above are all very similar, but may not be identical to Mac OS 10.2.

1. Pull down the Apple Menu. Click System Preferences and select Network.
2. Make sure that Built-in Ethernet is selected in the Show field.
3. On the TCP/IP tab, select Using DHCP in the Configure field.
4. Close the TCP/IP dialog box.

6.5 | Verifying Your TCP/IP Connection

After installing the TCP/IP communication protocols and configuring an IP address in the same network as the Router, use the ping command to check if your computer has successfully connected to the Router. The following example shows how the ping procedure can be executed in an MS-DOS window. First, execute the ping command:

ping 192.168.2.1

If a message similar to the following appears:

**Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64**

...a communication link between your computer and the Router has been successfully established.

If you get the following message:

**Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.**

...there may be something wrong in your installation procedure.

Check the following items in sequence:

1. Is the Ethernet cable correctly connected between the Router and the computer? The LAN LED on the Router and the Link LED of the network card on your computer must be on.
2. Is TCP/IP properly configured on your computer? If the IP address of the Router is 192.168.2.1, the IP address of your PC must be from 192.168.2.2 - 254 and the default gateway must be 192.168.2.1. If you can successfully ping the Router you are now ready to connect to the Internet!

7 | Configuring Your Broadband VPN Router

Before you attempt to log into the web-based Administration, please verify the following.

1. Your browser is configured properly (see below).
2. Disable any firewall or security software that may be running.
3. Confirm that you have a good link LED where your computer is plugged into the Router. If you don't have a link light, then try another cable until you get a good link.

7.1 | Browser Configuration

Confirm your browser is configured for a direct connection to the Internet using the Ethernet cable that is installed in the computer. This is configured through the options/preference section of your browser.

You will also need to verify that the HTTP Proxy feature of your web browser is disabled. This is so that your web browser will be able to view the Router configuration pages. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer 5 or above (For Windows)

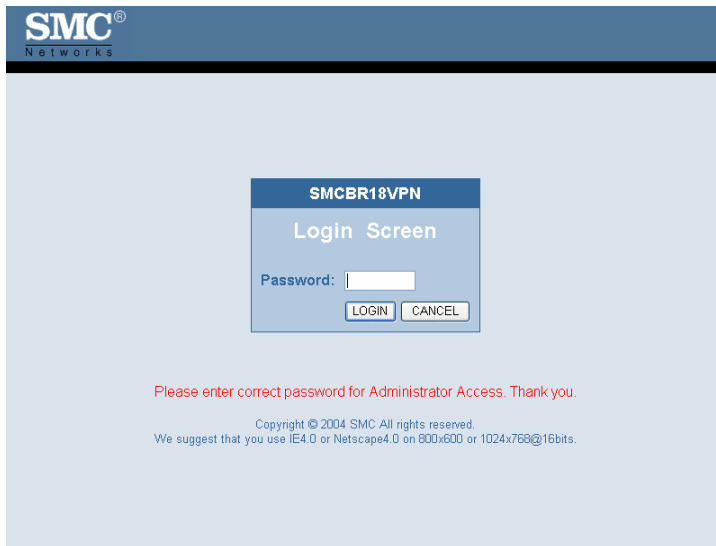
1. Open Internet Explorer. Click Tools, and then select Internet Options.
2. In the Internet Options window, click the Connections tab.
3. Click the LAN Settings button.
4. Clear all the check boxes and click OK to save these LAN settings changes.
5. Click OK again to close the Internet Options window.

Internet Explorer (For Macintosh)

1. Open Internet Explorer. Click Explorer/Preferences.
2. In the Internet Explorer Preferences window, under Network, select Proxies.
3. Uncheck all check boxes and click OK.

7.2 | Web Management

To access the Router's management interface, enter the Router IP address in your web browser <http://192.168.2.1>.



Note that there are two different Web user interfaces, one for general users and one for the system administrator. To log on as an administrator, enter the system password (default password is **smcadmin**) and click the **LOGIN** button. If you typed the password correctly, the left panel of the Web user interface changes to the administrator configuration mode as shown in the following figures.

7.3 | Setup Wizard

Time Zone

After logging into the web management, click on SETUP WIZARD on the top left navigation panel. The first item is Time Zone. For accurate timing of client filtering and log events, you need to set the time zone. Select your time zone from the drop-down list.




Broadband Type

The following screen lets you select a WAN type. Click one of the five options and then click [Next].

Fixed-IP xDSL

Some xDSL Internet Service Providers may assign a fixed (static) IP address. If you have been provided with this information, choose this option and enter the assigned IP address, gateway IP address, DNS IP addresses, and subnet mask.

3. IP Address Information

 **Fixed-IP xDSL**

Enter the IP address, Subnet Mask, Gateway IP address, and DNS IP address provided to you by your ISP in the appropriate fields above.

IP Address :	<input type="text" value="0.0.0.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway Address :	<input type="text" value="0.0.0.0"/>
Primary DNS Server :	<input type="text" value="0.0.0.0"/>
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>

PPPoE xDSL

Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Leave the Maximum Transmission Unit (MTU) at the default value unless you have a particular reason to change it. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. (Default: 10) Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.

3. IP Address Information



PPPoE xDSL

Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a Service Name enter it in the "Service Name" field, otherwise, leave it blank.

User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Service Name :	<input type="text"/>
MTU :	<input type="text" value="1492"/> (576<=MTU Value<=1492)
Maximum Idle Time (0-60) :	<input type="text" value="10"/> (minutes)
Connect mode:	<input type="radio"/> Always On Line <input type="radio"/> Manual Connect <input checked="" type="radio"/> Connect On Demand

PPTP


Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary.

If you have been provided with the information as shown on the screen, enter the assigned IP address, subnet mask, default gateway IP address, user ID and password, and PPTP Gateway. Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.

IP Mode :	Static IP Address ▼
PPTP Account :	<input type="text"/>
PPTP Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Service IP Address :	<input type="text"/>
My IP Address :	<input type="text"/>
My Subnet Mask :	255.255.255.0
WAN Gateway IP :	<input type="text"/>
Connection ID :	<input type="text"/>
MTU :	1460 (576-1460)
Maximum Idle Time (0-60) :	10 (minutes)
Connect mode:	<input type="radio"/> Always On Line <input type="radio"/> Manual Connect <input checked="" type="radio"/> Connect On Demand

BigPond

If you use the BigPond Internet Service which is available in Australia, enter your username and password and apply the changes.


BigPond

In this section you can configure the built-in client for the BigPond Internet service available in Australia.

User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Authentication Service Name :	<input type="text"/> (optional)

L2TP

Layer 2 Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary.

If you have been provided with the information as shown on the screen, enter the assigned IP address, subnet mask, default gateway IP address, user ID and password, and L2TP Gateway. Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it

will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.

IP Mode :	Static IP Address ▼
L2TP Account :	<input type="text"/>
L2TP Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
IP Address :	<input type="text"/>
Subnet Mask :	255.255.255.0
WAN Gateway IP :	<input type="text"/>
Server IP Address :	<input type="text"/>
MTU :	1462 (576-1462)
Maximum Idle Time (0-60) :	10 (minutes)
Connect mode:	<input type="radio"/> Always On Line <input type="radio"/> Manual Connect <input checked="" type="radio"/> Connect On Demand

Dial-Up

Most Dial-up users will select this option to connect to their ISP through an analog dial-up modem. This feature can be used as a back-up when your broadband connectivity is unavailable. Enter the phone number, account name and password assigned to you by your ISP. The baud rate is the communication rate between the broadband router and your modem. Set this to the desired rate. If you have received DNS addresses from your ISP, enter them here, otherwise leave these addresses at their default settings. The modem initialization string setting is most commonly used to optimize the communication quality between the ISP and your analog dial-up modem. If you are using the dial up modem as a backup, Enable the "Auto Backup/Failover" option. Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.



Dial-up Network

Dial-up Network WAN type.

Dial-up Phone Number :	<input type="text"/>
Dial-up Account :	<input type="text"/>
Dial-up Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Baud Rate :	57600 <input type="button" value="v"/> bps
Primary DNS :	<input type="text" value="0.0.0.0"/>
Secondary DNS :	<input type="text" value="0.0.0.0"/>
Assigned IP Address :	<input type="text" value="0.0.0.0"/> (optional)
Modem Initialization String :	<input type="text"/>
Maximum Idle Time (0-60) :	<input type="text" value="10"/> (minutes)
Auto Backup/Failover :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Connect mode:	<input type="radio"/> Always On Line <input type="radio"/> Manual Connect <input checked="" type="radio"/> Connect On Demand

7.4 | Advanced Setup - SYSTEM

Time Zone

Use the section below to configure the Barricade's system time. Select your timezone and configure the daylight savings option based on your location. This information is used for the time/date parental rules you can configure with the Barricade's Advanced Firewall. This information is also used for your network logging.

Once you set you time zone, you can automatically update the Barricade's internal clock by synchronizing with a public time server over the Internet. To configure this setting, choose one of the options below - each option allows a different method of updating.

Set your Local Timezone Settings			
Time Zone :	(GMT-08:00)Pacific Time (US & Canada): Tijuana ▼		
Daylight Savings :	<input type="checkbox"/> - Enable Auto Update feature		
Starts on :	January ▼	01 ▼	
Ends on :	January ▼	01 ▼	
● Get Date and Time by online Time Servers (NTP)			
Pre-set Servers :	time.nist.gov ▼		
Custom Server :	<input type="text"/>		<input type="button" value="Sync Now !"/>
● Set Date and Time using PC's Date and Time			
Computer Time/Date :	<input type="text" value="Wednesday, July 21, 2004 6:05:29 AM"/>		
● Set Date and Time manually			
Date :	Year: 2004 ▼	Month: June ▼	Day: 01 ▼
Time :	Hour: 0 (0-23)	Minute: 0 (0-59)	Second: 0 (0-59)

Password Settings

Use this section to configure the 2 password accounts and idle time-out setting for your Barricade Router. There are 2 levels of admin access for this VPN Router:

The Administrator account has Read/Write permission to view and change any settings. The default password for this account is "smcadmin".

The User account has Read-Only permissions to view but not change the settings. The default password for this account is "password".

Administrator Password Options	
Current Password :	<input type="text"/>
New Password :	<input type="text"/>
Confirm New Password :	<input type="text"/>

User Password Options	
Current Password :	<input type="text"/>
New Password :	<input type="text"/>
Confirm New Password :	<input type="text"/>

Idle Time Out Settings	
Idle Time Out :	<input type="text" value="10"/> Mins (Idle Time =0 : NO Time Out)

Remote Management

Use this section to configure the remote management feature of your Barricade Router so the web-management can be accessed from the Internet (WAN). You can restrict access to a single IP or a range of IP addresses. If the specified IP address is 0.0.0.0, any host can connect to the router to perform these tasks. You can use the subnet mask bits' /nn notation to specify a group of trusted IP addresses. For example, 10.1.2.0/24. You can also change the remote port that the administrator uses to gain access to the web management.

Remote Management :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Allow Access to :	<input checked="" type="radio"/> Any IP Address <input type="radio"/> Single IP : <input type="text"/> <input type="radio"/> IP Range : <input type="text"/> ~ <input type="text"/>
Remote Management Port :	<input type="text" value="8080"/>

Syslog Server

The Syslog Server tool will automatically download the Barricade log to the server IP address specified by the user. Enter the Server LAN IP Address and select the Enable radio button to enable this function. The broadband router is also able to send the log files to a specific email address. Simply enter the IP address of your mail server in the SMTP Server box, enter the email addresses of the recipients who will receive the email log, and put in your username and password. Note that you can also customize the subject title of the email! Check to be sure the radio button for Enable is checked and then submit the changes.

Syslog Server Options	
Syslog Server :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Address :	192.168.2. <input type="text"/>

E-MAIL Settings	
E-mail Alert :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="button" value="Send Mail Now"/>
SMTP Server IP/Port :	<input type="text"/>
E-mail addresses :	<input type="text"/>
E-mail Subject :	<input type="text"/>
User name :	<input type="text"/>
Password :	<input type="text"/>

Log Type Settings	
Log Type :	<input checked="" type="checkbox"/> System Activity <input checked="" type="checkbox"/> Debug Information <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Dropped Packets <input checked="" type="checkbox"/> Notice

7.5 | Advanced Setup - WAN

Dynamic IP

The cable modem option allows you to configure a host name and MAC Address. The Host Name is optional, but may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the Router. Use this address when registering for Internet service, and do not change it unless required by your ISP. If your ISP used the MAC address of an Ethernet card as an identifier when first setting up your broadband account, only connect the PC with the registered MAC address to the Router and click the Clone MAC Address button. This will replace the current Router MAC address with the already registered Ethernet card MAC address. If you are unsure of which PC was originally set up by the broadband technician, call your ISP and request that they register a new MAC address for your account. Register the default MAC address of the Router.

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: SETUP WIZARD, SYSTEM, WAN, LAN, NAT, FIREWALL, VPN, and ADVANCED. The main content area is titled "Dynamic IP" and contains the following text:

The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the Barricade.

If required by your Service Provider, you use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.

If necessary, you can use the "Release" and "Renew" buttons on the Status page to release and renew the WAN IP address.

Below the text, there is a form with two input fields and a button:

Host Name :	<input type="text"/>
MAC Address :	<input type="text" value="00-50-18-21-B2-73"/>
<input type="button" value="Clone MAC Address"/>	

PPPoE

Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Leave the Maximum Transmission Unit (MTU) at the default value unless you have a particular reason to change it. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. (Default: 10) Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.

User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Service Name :	<input type="text"/>
MTU :	<input type="text" value="1492"/> (576<=MTU Value<=1492)
Maximum Idle Time (0-60) :	<input type="text" value="10"/> (minutes)
Connect mode:	<p><input type="radio"/> Always On Line</p> <p><input type="radio"/> Manual Connect</p> <p><input checked="" type="radio"/> Connect On Demand</p>

PPTP

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary.

If you have been provided with the information as shown on the screen, enter the assigned IP address, subnet mask, default gateway IP address, user ID and password, and PPTP Gateway. Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.

IP Mode :	Static IP Address ▼
PPTP Account :	<input type="text"/>
PPTP Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Service IP Address :	<input type="text"/>
My IP Address :	<input type="text"/>
My Subnet Mask :	255.255.255.0
WAN Gateway IP :	<input type="text"/>
Connection ID :	<input type="text"/>
MTU :	1460 (576-1460)
Maximum Idle Time (0-60) :	10 (minutes)
Connect mode:	<input type="radio"/> Always On Line <input type="radio"/> Manual Connect <input checked="" type="radio"/> Connect On Demand

Static IP

Some Internet Service Providers may assign a fixed (static) IP address. If you have been provided with this information, choose this option and enter the assigned IP address, gateway IP address, DNS IP addresses, and subnet mask.

IP Address :	<input type="text" value="0.0.0.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway Address :	<input type="text" value="0.0.0.0"/>
Primary DNS Server :	<input type="text" value="0.0.0.0"/>
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>

BigPond

If you use the BigPond Internet Service which is available in Australia, enter your username and password and apply the changes.

User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Authentication Service Name :	<input type="text"/> (optional)

L2TP

Layer 2 Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary.

If you have been provided with the information as shown on the screen, enter the assigned IP address, subnet mask, default gateway IP address, user ID and password, and L2TP Gateway. Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.

IP Mode :	Static IP Address ▼
L2TP Account :	<input type="text"/>
L2TP Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
IP Address :	<input type="text"/>
Subnet Mask :	255.255.255.0
WAN Gateway IP :	<input type="text"/>
Server IP Address :	<input type="text"/>
MTU :	1462 (576-1462)
Maximum Idle Time (0-60) :	10 (minutes)
Connect mode:	<input type="radio"/> Always On Line <input type="radio"/> Manual Connect <input checked="" type="radio"/> Connect On Demand

Dial Up

Most Dial-up users will select this option to connect to their ISP through an analog dial-up modem. This feature can be used as a back-up when your broadband connectivity is unavailable. Enter the phone number, account name and password assigned to you by your ISP. The baud rate is the communication rate between the broadband router and your modem. Set this to the desired rate. If you have received DNS addresses from your ISP, enter them here, otherwise leave these addresses at their default settings. The modem initialization string setting is most commonly used to optimize the communication quality between the ISP and your analog dial-up modem. If you are using the dial up modem as a backup, Enable the "Auto Backup/Failover" option. Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.

Dial-up Phone Number :	<input type="text"/>
Dial-up Account :	<input type="text"/>
Dial-up Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Baud Rate :	57600 <input type="button" value="v"/> bps
Primary DNS :	<input type="text" value="0.0.0.0"/>
Secondary DNS :	<input type="text" value="0.0.0.0"/>
Assigned IP Address :	<input type="text" value="0.0.0.0"/> (optional)
Modem Initialization String :	<input type="text"/>
Maximum Idle Time (0-60) :	<input type="text" value="10"/> (minutes)
Auto Backup/Failover :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Connect mode:	<input type="radio"/> Always On Line <input type="radio"/> Manual Connect <input checked="" type="radio"/> Connect On Demand

7.6 | Advanced Setup - LAN

This is the local IP address of the router. All networked computers must use the LAN IP address of the router as their default Gateway. However, if necessary, it can be changed. Here you can configure the LAN IP address for the router and enable/disable the DHCP server for dynamic client address allocation. You can change the lease time if necessary as well. By default this is set to "One Week". The other options are Half Hour, One Hour, Two Hours, Half Day, One Day, Two Days, and Forever. "Forever" signifies that there is no time limit on the IP address lease.

For the IP address pool, a dynamic IP address range may be specified (Default: 192.168.2.100-199). Once the IP addresses, e.g. 192.168.2.100-199, have been assigned, these IP addresses will be part of the dynamic IP address pool. IP addresses from 192.168.2.2-99, and 192.168.2.200-254 will be available as static IP addresses. Remember not to include the address of the Router in the client address pool. Also remember to configure your client PCs for dynamic IP address allocation. Lastly, you can enter a local domain suffix in the Domain Name field.

> SETUP WIZARD	<h3>LAN Settings</h3> <p>You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on sp or protocols. The Barricade must have an IP address for the local network.</p>
SYSTEM	
WAN	
LAN	
> Client List	
NAT	
FIREWALL	
VPN	
ADVANCED	
DDNS	
UPnP	
TOOLS	
STATUS	

LAN IP Settings	
IP Address :	192.168.2.1
Subnet Mask :	255.255.255.0
DHCP Server Settings	
DHCP Server :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Lease Time :	One Week ▼
Start IP Address pool :	192.168.2.100
End IP Address pool :	192.168.2.199
Domain Name :	
More...	

You also have the option to configure more advanced settings by clicking the “More” button. You can configure the router’s DHCP server to give out specific Primary and Secondary DNS, Primary and Secondary WINS, and an alternate Gateway (in the event that the router is not the Internet gateway).

Start IP Address pool :	192.168.2.100
End IP Address pool :	192.168.2.199
Domain Name :	
Primary DNS :	0.0.0.0
Secondary DNS :	0.0.0.0
Primary WINS :	0.0.0.0
Secondary WINS :	0.0.0.0
Gateway :	0.0.0.0

Clicking on the “Client List” link brings up the DHCP Client Table, showing all the clients that have obtained DHCP addresses from the router:

» SETUP WIZARD

SYSTEM

WAN

LAN

» Client List

NAT

FIREWALL

VPN

ADVANCED

DDNS

UPnP

TOOLS

STATUS

DHCP Client List

IP Address	Host Name	MAC Address	Select
192.168.2.146	sotec	00-40-45-11-20-77	<input type="checkbox"/>

Wake up

Delete

Refresh

VPN Connection List

VPN Tunnel Name	VPN Protocol	Auth. Protocol	Action
-----------------	--------------	----------------	--------

Back

Refresh

7.7 | Advanced Setup - NAT

7.7.1 | Virtual Server

The firewall of the router filters out unrecognized packets to protect your intranet. This means that all network hosts are invisible to the outside world. However, some of the hosts can be made accessible by enabling the Virtual Server mapping. A virtual server is defined as a Service Port. All requests to this port will be redirected to the computer specified by the Server IP.

The virtual server can work with scheduling rules as well. This gives you more flexibility for access control.

» SETUP WIZARD

SYSTEM

WAN

LAN

NAT

» Virtual Server

» Special Applications

» Virtual Computer

FIREWALL

VPN

ADVANCED

DDNS

UPnP

TOOLS

STATUS

Virtual Server

You can configure the Barricade as a virtual server so that remote users accessing services such as the Web or FTP at you via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words on the requested service (TCP/UDP port number), the Barricade redirects the external service request to the appropriate server at another internal IP address).

Well known services :

- select one -

Schedule rule :

(00)Always

Copy to

ID -

ID	IP Address	Public Port/s	Private Port/s	Data Type	Enable	Use Rule#
1	192.168.2.			TCP	<input type="checkbox"/>	0
2	192.168.2.			TCP	<input type="checkbox"/>	0
3	192.168.2.			TCP	<input type="checkbox"/>	0
4	192.168.2.			TCP	<input type="checkbox"/>	0
5	192.168.2.			TCP	<input type="checkbox"/>	0
6	192.168.2.			TCP	<input type="checkbox"/>	0

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, you need to specify the following virtual server mapping as shown in the table below:

Service Port	Server IP	Enable
21	192.168.123.1	X
80	192.168.123.2	X
1723	192.168.123.6	X

The “IP Address” section should contain the IP of the server computer in the LAN network that will be providing the virtual services. The “Public Port” is the port number or port range on the WAN side that will be used to access the virtual service. The “Private Port” is the port number of the service used by the server computer. “Data Type” can be User Datagram Protocol (UDP), Transmission Control Protocol (TCP) or both. This depends on the type of service you are running. TCP is connection-oriented protocol and UDP is connectionless. Since most services are connection-oriented, you will most likely need to select TCP. For example, FTP and HTTP are connection-oriented services while DNS and many streaming radio servers are connectionless.

7.7.2 / Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, and Internet telephony. These applications cannot work with a pure NAT router because of the firewall function. However, the Special Applications feature allows some of these applications to work with the router. Should the Special Applications feature fail to make an application work, you can try setting your computer as a DMZ host.

Trigger: This is the outbound port number issued by the application.

Incoming Ports: When the trigger packet is detected, the inbound packets sent to specified port numbers are allowed to pass through the firewall.

The router provides some predefined settings. To add a predefined setting to your list, select an application and click “Copy to”.

Note: Only one computer can use the Special Application tunnels at any given time.

Popular applications : select one Copy to ID

select one ing Port/s Data Type Enable

TCP select one TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

TCP TCP ☐

For a full list of ports and the services that run on them, see <http://www.iana.org/assignments/port-numbers>

7.7.3 / Virtual Computer

Use the “Virtual Computer” option to maintain the privacy and security of the local network. Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

ID	Global IP	Local IP	Enable
1	<input type="text"/>	192.168.2. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.2. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.2. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.2. <input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.2. <input type="text"/>	<input type="checkbox"/>

7.8 | Advanced Setup - FIREWALL

7.8.1 / Network Filters

The VPN Broadband Router firewall includes comprehensive Outbound and Inbound Network Packet Filters. The firewall does not significantly affect system performance. The packet filter lets you control which packets are allowed to pass through the router. The Outbound Filter applies to all outbound packets. The Inbound Filter applies only to packets addressed to a virtual server or DMZ host.

You can select one of the two filtering policies:

- Allow all to pass except those that match the specified rules
- Deny all to pass except those that match the specified rules

The screenshot shows the 'Outbound Network Filter' configuration window. On the left is a sidebar with a 'SETUP WIZARD' menu and various system settings like SYSTEM, WAN, LAN, NAT, FIREWALL, and ADVANCED. The main area is titled 'Outbound Network Filter' and contains the following options:

- Outbound Filter:** Radio buttons for 'Enable' and 'Disable' (selected).
- Schedule rule:** A dropdown menu set to '(00)Always' and a 'Copy to ID' button.
- Policy:** Radio buttons for 'ALLOW all network traffic except for the rules listed below' (selected) and 'BLOCK / DENY all network traffic except for the rules listed below'.
- Buttons:** 'Inbound Filter...' and 'MAC Level...'.

Below these options is a table with 5 columns: ID, Source IP : Ports, Destination IP : Ports, Enable, and Use Rule#. The table contains 5 rows of empty input fields for configuring rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1			<input type="checkbox"/>	0
2			<input type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0

You can apply up to 8 rules for each direction, inbound or outbound. For each rule you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP, or both
- Use Rule #

You can define a single IP address (4.3.123.254) or a range of IP addresses (4.3.123.254 - 4.3.2.254) for the source or destination IP address. A blank IP implies that all IP addresses are included. You can define a single port (80) or a range of ports (1000 - 1999) for the source or destination port. Specify the TCP or UDP protocol by adding the prefix T or U. Not adding a prefix implies all ports. Each rule can be enabled or disabled.

7.8.2 / URL Blocking

URL Blocking blocks LAN computers from accessing pre-defined Websites. The difference between the Domain Filter and URL Blocking is that the Domain filter requires you to enter a suffix (.com or .org), while URL Blocking requires you to enter only a keyword. In other words, the Domain Filter can block specific Websites, while URL Blocking can block hundreds of Websites simply by using a keyword.

- URL Blocking: Check the box next to Enable if you want to enable the URL Blocking option.
- URL / Keyword: If any part of a Website's URL matches the pre-defined word you have entered here, the connection will be blocked. For example, if you type the word "firewall" into the URL text field, all URLs containing that word will be blocked.
- Enable: Check the box to enable the rules.
- Use Rule #: Applies a configured schedule rule

URL Blocking

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword.

Schedule rule : (00)Always ID -

Rule Number	URL / Keyword	Enable	Use Rule#
Site 1	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 2	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 3	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 4	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 5	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 6	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 7	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 8	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Site 9	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

7.8.3 / MAC Filter

MAC Address Filtering allows you assign different access rights to various users and you can also assign a specific IP address to a certain MAC address.

Select the Enable radio button to enable the MAC Address Control. All of the settings on this screen take effect when Enable is checked.

- **MAC Address:** This is the unique address of a specific client.
- **IP Address:** Expected IP address of the corresponding client. You can keep this text field blank if you do not know the address.

The DHCP pull-down menu lets you select specific clients.

Select clients from the DHCP clients list and click "Copy to", to copy the MAC addresses to the selected ID, chosen from the ID pull-down menu.

- **Previous Page / Next Page:** Use these links to navigate to different pages. The router supports up to 32 MAC filters.

MAC Address Control :		<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
		<input type="radio"/> ALLOW these clients access to your network <input checked="" type="radio"/> BLOCK / DENY these clients access to your network	
DHCP Client List :		- select one - 00-40-45-11-20-77 : 192.168.2.146 [sotec]	Copy to ID - - select one -

ID	Computer Name	IP Address	MAC Address
1	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>
2	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>
3	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>
4	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>
5	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>

7.8.4 / Schedule Rule

Set scheduled times to be used to control what time of day a service or set of services is enabled. Use this section to configure up to 10 Schedule Rules to limit network access based on time and day. To create a schedule rule click the [Add Schedule Rule...] link below.

Schedule : <input type="radio"/> Enable <input checked="" type="radio"/> Disable		
--	--	--

Rule#	Rule Name	Configure
No Valid Schedule Rule !!!		

[Add Schedule Rule...](#)

Enter a rule name into the text field next to "Name of Rule 1". Click Save Settings to save your settings.

Edit Schedule Rule 1

Use this section to configure the details for the Schedule Rule. The military time format is used to configure the time for a schedule rule. For example 2:00PM is entered as 14:00.

Name of Rule 1 : <input type="text"/>		
Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>

The Schedule Rule screen appears. It now shows your setting for Rule 1. If you need to make changes to your setting, click the Edit button. If you want to delete Rule 1, click the Delete button.

Schedule : <input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Rule#	Rule Name	Configure
1	sample	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

[Add Schedule Rule...](#)

7.8.5 / Advanced

In this section you can enable/disable Stateful Packet Inspection (SPI), Discard Ping from WAN, and PPTP and IPSec VPN Passthrough types.

When Discard Ping From WAN is enabled, computers on the Internet will not get a reply back from the VPN Broadband Router when it is being "ping"ed. This may help to increase security.

When SPI is enabled, the router will extensively record specific packet information passed through the router such as IP address, port address, ACK, and so on. The router will also check every incoming packet to detect its validity.

FIREWALL Options	
SPI mode :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Discard Ping From WAN :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

VPN Passthrough	
PPTP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPSec :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

7.8.6 / DMZ

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

DMZ Host :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Address :	192.168.2. <input type="text"/>

7.9 | Advanced Setup - VPN

7.9.1 / IPSec Tunnel

VPN settings are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information, by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

» SETUP WIZARD

SYSTEM

WAN

LAN

NAT

FIREWALL

VPN

» VPN Settings

» PPTP Server

» L2TP Server

ADVANCED

DDNS

UPnP

TOOLS

STATUS

VPN Settings

VPN Settings are used to create virtual private tunnels to remote VPN gateways.

VPN :

☐ Enable
☒ Disable

NetBIOS broadcast :

☐ Enable
☒ Disable

Max. number of tunnels :

0

[Previous page](#)
[Next page](#)
[\[Dynamic VPN\]...](#)

ID	Tunnel Name	Method
1		IKE <input type="button" value="More"/>
2		IKE <input type="button" value="More"/>
3		IKE <input type="button" value="More"/>
4		IKE <input type="button" value="More"/>
5		IKE <input type="button" value="More"/>

- **VPN:** VPN protects network information from intruders. However, it greatly decreases network throughput. Enable it only when a security tunnel is absolutely necessary. This feature is disabled by default.
- **Max. Number of Tunnels:** Set the number of tunnels that are allowed to be in operation simultaneously.
- **Tunnel name:** Lists the monitored tunnel.
- **Method:** IPSec VPN supports two kinds of key-exchange methods: manual key exchange and the automatic key exchange. The manual key exchange method indicates that the authenticator and the encryption key of the two end VPN gateways are setup manually by the system managers. However, the IKE method performs an automatic Internet key exchange. The system managers of both end gateways only need to set the same pre-shared key.
- **“More” button:** Click the “More” button to setup detailed configuration for Manual key or IKE methods.

There are three settings that must be configured to enable IKE for a dedicated tunnel:

- Basic setup
- IKE proposal setup
- IPSec proposal setup

Basic Setup

- **Local Subnet:** The subnet of the local VPN gateway’s LAN site. The subnet can be a host, a partial subnet, or the whole subnet of the local gateway’s LAN site.
- **Local netmask:** The local netmask combined with the local subnet forms a subnet domain.
- **Remote subnet:** The subnet of a remote VPN gateway’s LAN site. The subnet can be a host, a partial subnet, or the whole subnet of the remote gateway’s LAN site.
- **Remote netmask:** The remote netmask combined with the remote subnet forms a subnet domain.
- **Remote gateway:** The IP address of the remote gateway.
- **Pre-shared key:** The first key that supports the IKE mechanism of both VPN gateways to negotiate further security keys. The pre-shared key must be the same for both end gateways.

Options

- Select IKE proposal: Click this button to setup a set of frequently used IKE proposals for the dedicated tunnel.
- Select IPSec proposal: Click this button to setup a set of frequently used IPSec proposals for the dedicated tunnel.

The tunnel name is equal to the name you configured on the previous page of VPN settings. The IKE proposal index includes the settings for a set of frequently used IKE proposals and offers a selection of the IKE proposals. The IPSec proposal index includes the settings for a set of frequently used IPSec proposals and offers a selection of the IPSec proposals.

VPN Settings - Tunnel 1 - IKE

Tunnel 1 - IKE	
Tunnel Name	<input type="text" value="sample"/>
Aggressive Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Local Subnet	<input type="text" value="0.0.0.0"/>
Local Netmask	<input type="text" value="0.0.0.0"/>
Remote Subnet	<input type="text" value="0.0.0.0"/>
Remote Netmask	<input type="text" value="0.0.0.0"/>
Remote Gateway	<input type="text"/>
Preshare Key	<input type="text"/>
IKE Proposal index	<input type="button" value="Select IKE Proposal..."/>
IPSec Proposal index	<input type="button" value="Select IPSec Proposal..."/>

7.9.2 / IKE Proposal

- IKE Proposal index: A list of selected proposal indexes from the IKE proposal pool. The selected activity is performed when you select a proposal ID and click the Add to button next to the Proposal ID roll-down list. A maximum of four indexes can be selected from the proposal pool for the dedicated tunnel.
- Proposal Name: The proposal name indicates which IKE proposal will be monitored. The first character of the name with the value of 0x00 stands for the IKE proposal that is not available.
- DH Group - Three groups can be selected:
 - Group 1 (MODP768)
 - Group 2 (MODP1024)
 - Group 5 (MODP1536)
- Encryption algorithm - Two algorithms can be selected:
 - 3DES
 - DES
- Authentication algorithm - Two algorithms can be selected:
 - SHA1

- MD5
- Life Time: The unit of Life time is based on the value of the life time unit, which can be seconds or KB. If the value of the unit is seconds, the value of life time represents the life time of the dedicated VPN tunnel between both end gateways. Its value can range from 300 to 172,800 seconds. If the value of the unit is KB, the value of life time represents the maximum allowable amount of transmitted packets through the dedicated VPN tunnel between both end gateways. This value can range from 20,480 to 2,483,647 KB.
- Life Time Unit: The life time unit can be set to seconds or KB.
- Proposal ID: The identifier of the IKE proposal can be selected for adding a corresponding proposal to the dedicated tunnel. A total of ten proposals can be set in the proposal pool. A maximum of four proposals from the pool can be applied to the dedicated tunnel.
- "Add to" button: Click this button to add the selected proposal, shown in the proposal ID field of the IKE Proposal index list. The proposal shown in the index list will be used in phase 1 of the IKE negotiation for obtaining the IKSAMP SA of the dedicated tunnel.

VPN Settings - Tunnel 1 - Set IKE Proposal

IKE Proposal index

- Empty -

Remove

Proposal ID :

- select one - ▼

Add to

Proposal index

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	<input style="width: 80px;" type="text"/>	Group 1 ▼	3DES ▼	SHA1 ▼	<input style="width: 40px;" type="text" value="0"/>	Sec. ▼
2	<input style="width: 80px;" type="text"/>	Group 1 ▼	3DES ▼	SHA1 ▼	<input style="width: 40px;" type="text" value="0"/>	Sec. ▼
3	<input style="width: 80px;" type="text"/>	Group 1 ▼	3DES ▼	SHA1 ▼	<input style="width: 40px;" type="text" value="0"/>	Sec. ▼
4	<input style="width: 80px;" type="text"/>	Group 1 ▼	3DES ▼	SHA1 ▼	<input style="width: 40px;" type="text" value="0"/>	Sec. ▼
5	<input style="width: 80px;" type="text"/>	Group 1 ▼	3DES ▼	SHA1 ▼	<input style="width: 40px;" type="text" value="0"/>	Sec. ▼

7.9.3 / IPSec Proposal

- IPSec Proposal index: A list of selected proposal indexes from the IPSec proposal pool. The selected activity is performed when you select a proposal ID and click the Add to button next to Proposal ID roll-down list. A maximum of four indexes can be selected from the proposal pool for the dedicated tunnel.

- **Proposal Name:** The proposal name indicates which IPSec proposal will be monitored. The first character of the name with the value of 0x00 stands for the IPSec proposal that is not available.
- **DH Group** - Three groups can be selected:
 - Group 1 (MODP768)
 - Group 2 (MODP1024)
 - Group 5 (MODP1536)
 However, you can also select None.
- **Encapsulation protocol** - Two protocols can be selected:
 - ESP
 - AH
- **Encryption algorithm** - Two algorithms can be selected:
 - 3DES
 - DES
 However, when the encapsulation protocol is set to AH, the encryption algorithm is unnecessary.
- **Authentication algorithm** - Two algorithms can be selected:
 - SHA1
 - MD5
 However, you can also select None.
- **Life Time:** The unit of Life time is based on the value of the life time unit, which can be seconds or KB. If the value of the unit is seconds, the value of life time represents the life time of the dedicated VPN tunnel between both end gateways. Its value can range from 300 to 172,800 seconds. If the value of the unit is KB, the value of life time represents the maximum allowable amount of transmitted packets through the dedicated VPN tunnel between both end gateways. This value can range from 20,480 to 2,483,647 KB.
- **Life Time Unit:** The life time unit can be set to seconds or KB.
- **Proposal ID:** The identifier of the IPSec proposal can be selected for adding a corresponding proposal to the dedicated tunnel. A total of ten proposals can be set in the proposal pool. A maximum of four proposals from the pool can be applied to the dedicated tunnel.
- **"Add to" button:** Click this button to add the selected proposal, shown in the proposal ID field of the IPSec Proposal index list. The proposal shown in the index list will be used in phase 2 of the IPSec negotiation for getting the IPSec SA of the dedicated tunnel.

VPN Settings - Tunnel 1 - Set IPSec Proposal

IPSec Proposal index	<div>- Empty -</div> <div>Remove</div>						
Proposal ID :	<div>- select one -</div> <div>Add to</div> <div>Proposal index</div>						

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	<input type="text"/>	None ▾	ESP ▾	3DES ▾	None ▾	0	Sec. ▾
2	<input type="text"/>	None ▾	ESP ▾	3DES ▾	None ▾	0	Sec. ▾
3	<input type="text"/>	None ▾	ESP ▾	3DES ▾	None ▾	0	Sec. ▾
4	<input type="text"/>	None ▾	ESP ▾	3DES ▾	None ▾	0	Sec. ▾
5	<input type="text"/>	None ▾	ESP ▾	3DES ▾	None ▾	0	Sec. ▾

7.9.4 / Dynamic VPN

When using the VPN Dynamic IP Setting, the router functions as a Dynamic VPN server. The Dynamic VPN server does not check the VPN client IP information - this means that you can build a VPN tunnel with a VPN gateway from any remote host, regardless of the IP information.

VPN Settings - Dynamic VPN Tunnel

Dynamic VPN Tunnel Options	
Tunnel Name :	<input type="text"/>
Dynamic VPN :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Local Subnet :	<input type="text" value="0.0.0.0"/>
Local Netmask :	<input type="text" value="0.0.0.0"/>
Preshare Key :	<input type="text"/>
IKE Proposal index :	<div>Select IKE Proposal...</div>
IPSec Proposal index :	<div>Select IPSec Proposal...</div>

7.9.5 / PPTP/L2TP Server

Point-to-Point and Layer 2 Tunneling Protocols (PPTP / L2TP) allows the secure remote access over the Internet by simply dialing in a local point provided by an ISP. The following screen displays the management interface where you enter username and passwords for authorized remote users, the authentication protocol, and the IP address range to assign to those users:

PPTP Server

PPTP Server :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual IP of PPTP Server :	10 . 0 . 0 . 1
Authentication Protocol :	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP
MPPE Encryption Mode:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

ID	Tunnel Name	User Name	Password
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

The VPN Broadband Router supports PAP, CHAP and MS-CHAP authentication protocols. You can also enable or disable support MPPE which is a Microsoft standard Point-to-Point Encryption protocol. We recommend enabling MPPE at all times. However, please note that with MPPE enabled, the only supported authentication protocol is MS-CHAP. This is because during the MS-CHAP authentication process, shared secret encryption keys for Microsoft Point-to-Point Encryption (MPPE) are generated. This does not occur when using PAP or CHAP.

PAP is a simple authentication protocol where the username and password data are both handled in a cleartext or unencrypted format. We do not recommend using PAP because your passwords are easily readable from the Point-to-Point Protocol (PPP) packets exchanged during the authentication process.

When authenticating using Challenge Handshake Authentication Protocol (CHAP), the knowledge of the password, rather than the password itself is what is sent by the client. With CHAP, the VPN Broadband Router sends the remote client a challenge string. The remote client uses the challenge string and the password, and creates a Message Digest-5 (MD5) hash which is then forwarded to the VPN server. The VPN server computes the same hash calculation and compares the result with the hash sent by the client. If they match, the remote client is considered an authentic user.

Note: The virtual IP of the PPTP server and L2TP server must not conflict.

L2TP Server :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual IP of L2TP Server :	10 . 0 . 1 . 1
Authentication Protocol :	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP
MPPE Encryption Mode:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

ID	Tunnel Name	User Name	Password
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

7.10 | Advanced Setup - SNMP

The Simple Network Management Protocol (SNMP) lets you manage a computer network remotely by polling and setting terminal values and monitoring network events.

- **Enable SNMP:** You can check Local, Remote, or both options to enable the SNMP function.
 - If Local is checked, the router responds only to requests from the LAN.
 - If Remote is checked, the router responds only to requests from the WAN.
- **Get Community:** Setting this option allows the router respond to a request.
- **Set Community:** Setting this option allows your router to accept a request.

NAT	<div>SNMP Setting</div> <div>Enable SNMP : <input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote</div> <div>Get Community : <input type="text" value="public"/></div> <div>Set Community : <input type="text" value="private"/></div> <div>IP 1 : <input type="text"/></div> <div>IP 2 : <input type="text"/></div> <div>IP 3 : <input type="text"/></div> <div>IP 4 : <input type="text"/></div> <div>SNMP Version : <input type="radio"/> V1 <input checked="" type="radio"/> V2c</div>
FIREWALL	
VPN	
ADVANCED	
» SNMP	
» Routing	
» Miscellaneous	
» Display Status	
DDNS	
UPnP	
TOOLS	
STATUS	

7.11 | Advanced Setup - ROUTING

The Routing Table lets you determine which physical interface address to use for outgoing IP data grams. If you have more than one router and subnet, you will have to enable the routing table to allow packets to find the routing path. This allows different subnets to communicate with each other. The settings in the routing table are used to support static and dynamic routing functions. RIPv1 is a protocol where the IP address is routed through the Internet. RIPv2 is an enhanced version of RIP v1 with added features such as Authentication, Routing Domain, Next Hop Forwarding, and Subnetmask Exchange.

Dynamic Routing :		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
Static Routing :		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Enable Static Routing by selecting the radio button next to Enable.

- Static Routing: Allows you to specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by toggling the Enable check box. Once the routing table settings are configured, click Save.

packets to find proper routing path and allow different subnets to communicate with each other.

Dynamic Routing : ☒ Disable ☐ RIPv1 ☐ RIPv2

Static Routing : ☐ Disable ☒ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	192.168.3.0	255.255.255.0	192.168.1.33	1	<input checked="" type="checkbox"/>
2	192.168.5.0	255.255.255.0	192.168.1.56	1	<input checked="" type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>

HELP SAVE SETTINGS CANCEL

7.12 | Advanced Setup - MISCELLANEOUS

If you experience difficulties accessing an FTP server that is running on a port other than 21, you can enter that port in the "Non-standard FTP port" and apply the changes.

Wake-on-LAN is a technology that lets you power up a networked router remotely. To use this feature, the target network adapter must be Wake-on-LAN enabled and you have to know the MAC address of the adapter. The address should look similar to this: 00-11-22-33-44-55. Depressing the "Wake up" button tells the router to send the wake-up frame to the target adapter.

Miscellaneous Options

Non-standard FTP port :

MAC Address for Wake-on-LAN : Wake up

Domain Name or IP address for Ping Test : Ping

The ping diagnostics feature allows you to configure an IP address to ping from the router. You can ping a specific IP or domain to test whether the router is active.

7.13 | Advanced Setup - DISPLAY STATUS

Enable the Display Status option to view the WAN connectivity settings on the login page.

When this is enabled, the login page appears as follows:

7.14 | DDNS (Dynamic DNS)

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes. Before you can enable the Dynamic DNS, you need to register an account with one of the Dynamic DNS servers that are listed in the Provider field.

Dynamic DNS : <input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Service Configuration	
DDNS Service :	DynDNS.org(Dynamic) ▼
Domain Name :	DynDNS.org(Dynamic) DynDNS.org(Custom) <input type="text"/>
Username / E-mail :	TZO.com No-IP.com <input type="text"/>
Password / Key :	<input type="text"/>
Server Configuration	
Server IP :	192.168.2. <input type="text"/>
Server Type :	Web Server: (HTTP) Port 80 <input type="checkbox"/> Port 8000 <input type="checkbox"/> FTP Server: Port 20 <input type="checkbox"/> Port 21 <input type="checkbox"/> Email Server: (POP3) Port 110 <input type="checkbox"/> (SMTP) Port 25 <input type="checkbox"/>

7.15 | UPnP (Universal Plug-and-Play)

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity networking in addition to control and data transfer among networked devices in the home, office and everywhere in between.

Universal Plug and Play (UPnP) :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
----------------------------------	---

7.16 | Tools

The Toolbox menu allows you to view your system logs, upgrade firmware, backup settings, restore settings to defaults, reboot the router, and access miscellaneous settings.

SYSTEM

WAN

LAN

NAT

FIREWALL

VPN

ADVANCED

DDNS

UPnP

TOOLS

» Configuration Tools

» Firmware Upgrade

» Reboot

STATUS

Configuration Tools

Use the "Backup" tool to save the Barricade's current configuration to a file named "backup_config.exe" on your PC. You can then use the "Restore" tool to restore the saved configuration to the Barricade. Alternatively, you can use the "Restore to Factory Default" tool to force the Barricade to perform a power reset and restore the original factory settings.

Barricade Tool Options	
Backup Router Settings :	<input type="button" value="Backup to SMCrouter_backup.bin"/>
Restore Router Settings :	<input type="text"/> <input type="button" value="Browse..."/>
	<input type="button" value="Restore from config file.."/>
Reset Barricade to Factory Settings :	<input type="button" value="Reset to Default Settings"/>

7.17 | Status

You can use the Status screen to see the connection status for Barricade's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current time: Wed Jul 21, 2004 01:46:05 PM

Connection Status

DHCP Client Connected.
WAN IP: 10.10.2.96
Subnet Mask: 255.255.255.0
Gateway: 10.10.2.1
Primary DNS: 10.10.2.1
Secondary DNS: 0.0.0.0

Barricade Settings

IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
SPI Mode : Disabled
UPnP: Disabled
Numbers of DHCP Clients: 1

Hardware Information

Runtime Code Version: R1.00(Jul 20 2004)
Boot Code Version: R1.C321.89AB
LAN MAC Address: 00-50-18-21-B2-74
WAN MAC Address: 00-50-18-21-B2-73
Hardware Version: R1.00

Release

Renew

DHCP Client Log

[View DHCP clients.](#)

Name=sotec IP=192.168.2.146 Expire Date=Wed Jul 28 08:25:50 2004

Client List

Network Log

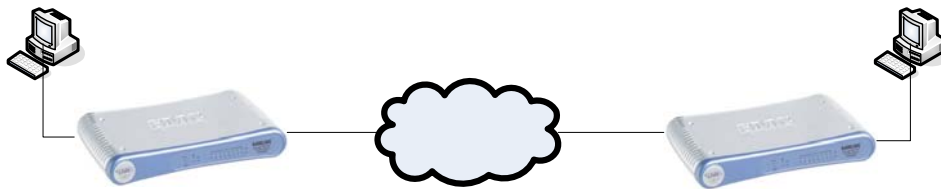
[View network activity and security logs.](#)

Wed Jul 21 06:27:20 2004 DHCP:offer(10.10.2.1)
Wed Jul 21 08:27:20 2004 DHCP:request(10.10.2.96)
Wed Jul 21 08:27:21 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 08:57:22 2004 DHCP:renew
Wed Jul 21 08:57:22 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 09:02:42 2004 Admin from 192.168.2.146 login successfully
Wed Jul 21 09:19:40 2004 Admin from 192.168.2.146 login successfully
Wed Jul 21 09:27:23 2004 DHCP:renew
Wed Jul 21 09:27:23 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 09:57:24 2004 DHCP:renew
Wed Jul 21 09:57:24 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 10:01:35 2004 Restarted by 192.168.2.146
Wed Jul 21 10:01:43 2004 DOD:TCP trigger from 192.168.2.146:1519 to 198.173.217.138:110

8 | IPSec Settings Guide (For Reference/Example Only)

8.1 | Tunnel between two SMCBR14VPN

The easiest way to construct a VPN tunnel between two sites is to use two SMCBR14VPNs, which are connected to the internet.



The steps to follow to create an IP tunnel between are the following:

- Step 1: Go to the VPN section and select the enable checkbox for [VPN]
- Step 2: Select the number of Tunnels you want to enable
- Step 3: Enter a Tunnel Name, select IKE or MANUAL for the method and click [More]
- Step 4: Local subnet value is the LAN SUBNET
- Step 5: Local netmask value is the LAN SUBNET MASK
- Step 6: Remote subnet value is the LAN SUBNET of the REMOTE NETWORK
- Step 7: Remote netmask value is the LAN SUBNET MASK of the REMOTE NETWORK
- Step 8: Remote gateway value is the WAN IP of the REMOTE NETWORK
- Step 9: Preshare key value is used to determine the network encryption
- Step 10: SAVE SETTINGS and then configure the IKE PROPOSAL and IPSEC PROPOSAL

8.1.1 | Settings for Router 1

VPN Router	WAN IP Address: ip1.smc.com
1	LAN IP Address: 192.168.1.1
PC	192.168.1.xxx

Intern

WAN IP: ip1.smc.com

SMC® Networks **ADVANCED SETUP** **SMCBR18VPN** Home Logout

SETUP WIZARD

SYSTEM

WAN

LAN

NAT

FIREWALL

VPN

> VPN Settings

> PPTP Server

> L2TP Server

ADVANCED

DDNS

UPnP

TOOLS

STATUS

VPN Settings

VPN Settings are used to create virtual private tunnels to remote VPN gateways.

VPN : ☒ Enable ☐ Disable

NetBIOS broadcast : ☐ Enable ☒ Disable

Max. number of tunnels : 2

[Previous page](#) [Next page](#) [\[Dynamic VPN\]...](#)

ID	Tunnel Name	Method
1	1	IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More
6		IKE More
7		IKE More

Set the VPN settings as follows:

VPN: Enable
 Max. number of tunnels: 2
 ID: 1
 Tunnel Name: 1
 Method: IKE

When finished, click "More".

VPN Settings - Tunnel 1 - IKE

Tunnel 1 - IKE	
Tunnel Name	1
Aggressive Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.2.0
Remote Netmask	255.255.255.0
Remote Gateway	ip2.smc.com
Preshare Key	mypresharedkey
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Set the Tunnel 1 IKE settings as follows:

Tunnel 1:	1
Local Subnet:	192.168.1.0
Local Netmask:	255.255.255.0
Remote Subnet:	192.168.1.0
Remote Netmask:	255.255.255.0
Remote Gateway:	ip2.smc.com
Preshare Key:	mypresharedkey

When finished, save your settings.

8.1.2 / Settings for router 2

VPN Router	WAN IP Address: ip2.smc.com
2	LAN IP Address: 192.168.2.1
PC	192.168.2.xxx

SMC® Networks **ADVANCED SETUP** **SMCBR18VPN** [Home](#) [Logout](#)

SETUP WIZARD

SYSTEM

WAN

LAN

NAT

FIREWALL

VPN

> VPN Settings

> PPTP Server

> L2TP Server

ADVANCED

DDNS

UPnP

TOOLS

STATUS

VPN Settings

VPN Settings are used to create virtual private tunnels to remote VPN gateways.

VPN : ☒ Enable ☐ Disable

NetBIOS broadcast : ☐ Enable ☒ Disable

Max. number of tunnels :

[Previous page](#) [Next page](#) [\[Dynamic VPN\]...](#)

ID	Tunnel Name	Method
1	<input type="text" value="1"/>	IKE <input type="button" value="More"/>
2	<input type="text"/>	IKE <input type="button" value="More"/>
3	<input type="text"/>	IKE <input type="button" value="More"/>
4	<input type="text"/>	IKE <input type="button" value="More"/>
5	<input type="text"/>	IKE <input type="button" value="More"/>
6	<input type="text"/>	IKE <input type="button" value="More"/>
7	<input type="text"/>	IKE <input type="button" value="More"/>

Set the VPN settings as follows:

VPN: Enable
 Max. number of tunnels: 2
 ID: 1
 Tunnel Name: 1
 Method: IKE

When finished, click "More".

VPN Settings - Tunnel 1 - IKE

Tunnel 1 - IKE	
Tunnel Name	<input type="text" value="1"/>
Aggressive Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Local Subnet	<input type="text" value="192.168.2.0"/>
Local Netmask	<input type="text" value="255.255.255.0"/>
Remote Subnet	<input type="text" value="192.168.1.0"/>
Remote Netmask	<input type="text" value="255.255.255.0"/>
Remote Gateway	<input type="text" value="ip1.smc.com"/>
Preshare Key	<input type="text" value="mypresharedkey"/>
IKE Proposal index	<input type="button" value="Select IKE Proposal..."/>
IPSec Proposal index	<input type="button" value="Select IPSec Proposal..."/>

Set the Tunnel 1 IKE settings as follows:

Tunnel 1:	1
Local Subnet:	192.168.2.0
Local Netmask:	255.255.255.0
Remote Subnet:	192.168.1.0
Remote Netmask:	255.255.255.0
Remote Gateway:	ip1.smc.com
Preshare Key:	mypresharedkey

When finished, save your settings.

8.1.3 / Common Settings for both routers

VPN Settings - Tunnel 1 - Set IKE Proposal

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	1	Group 2	3DES	SHA1	10000	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.

Set the Tunnel 1 IKE Proposal settings as follows:

ID: 1
Proposal Name: 1
DH Group: Group2
Encrypt. algorithm: 3DES
Auth. algorithm: SHA1
Life Time: 10000
Life Time Unit: Sec.

When finished, save the settings.

VPN Settings - Tunnel 1 - Set IPSec Proposal

SMC® Networks ADVANCED SETUP SMCBR18VPN Home Logout

> SETUP WIZARD

SYSTEM

WAN

LAN

NAT

FIREWALL

VPN

> VPN Settings

> PPTP Server

> L2TP Server

ADVANCED

DDNS

UPnP

TOOLS

STATUS

VPN Settings - Tunnel 1 - Set IPSec Proposal

IPSec Proposal index: - Empty - Remove

Proposal ID: -- select one -- Add to Proposal index

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	1	Group 2	ESP	DES	MD5	10000	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.

Set the Tunnel 1 IPSec Proposal settings as follows:

ID: 1
Proposal Name: 1
DH Group: Group2
Encap. protocol: ESP
Encrypt. algorithm: DES
Auth. Algorithm: MD5
Life Time: 10000
Life Time Unit: Sec.

When finished, save the settings.

Now to view the VPN connection process, go to the STATUS page and view the System Log.
Now PC1, with IP 192.168.1.100 has access to PC2, with IP 192.168.2.100

8.2 | Tunnel between a SMCBR14VPN and standalone client.

Alternatively, a tunnel can be established between a PC and SMCBR14VPN. The easiest way to this is to use an IPSEC VPN client software running at the PC. After configuring the client accordingly, the only change to the configuration is the remote mask, which in this case would be 255.255.255.255, as we are configuring a tunnel for only one client. If clients are connecting from various IPs, dynamic VPN is a good solution for this.

8.3 | PPTP/ L2TP configuration example

Please note that the virtual address of the L2TP and PPTP server have to be different.

PPTP

- Step 1: Go to the PPTP Server section and select the Enable radio button
- Step 2: Change the virtual IP value if necessary (this is the IP network that your PPTP clients will automatically be connected to)
- Step 3: Set the authentication protocol
- Step 4: Enter a tunnel name and set the username and password
- Step 5: Configure your remote VPN client to connect to the WAN IP of the router

PPTP Server

PPTP Server :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual IP of PPTP Server :	10 . 0 . 0 . 1
Authentication Protocol :	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP

ID	Tunnel Name	User Name	Password
1	<input type="text"/>	<input type="text"/>	<input type="text"/>

L2TP

Microsoft uses an embedded L2TP/IPSEC VPN implementation. In order to use the Microsoft standard VPN client, one has to disable the IPSEC on the PC. Please refer to Microsoft help to perform this operation.

- Step 1: Go to the L2TP Server section and select the Enable radio button
- Step 2: Change the virtual IP value if necessary (this is the IP network that your L2TP clients will automatically be connected to)
- Step 3: Set the authentication protocol
- Step 4: Enter a tunnel name and set the username and password
- Step 5: Configure your remote VPN client to connect to the WAN IP of the router

L2TP Server

L2TP Server :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual IP of L2TP Server :	<input type="text" value="10"/> . <input type="text" value="0"/> . <input type="text" value="1"/> .1
Authentication Protocol :	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP

ID	Tunnel Name	User Name	Password
1	<input type="text"/>	<input type="text"/>	<input type="text"/>

9 | Troubleshooting

A. Verifying your connection to the router

If you are unable to access the Router's web-based administration pages, then you may not be properly connected or configured.

To determine your TCP/IP configuration status please follow the steps below:

1. Click Start then choose Run.
2. Type cmd or command to open a DOS prompt.
3. In the DOS window, type ipconfig and verify the information that is displayed.
4. If your computer is set up for DHCP, then your TCP/IP configuration should be similar to the information displayed:
 - IP Address: 192.168.2.x (x is number between 100 and 199 by default.)
 - Subnet: 255.255.255.0
 - Gateway: 192.168.2.1

If you have an IP address that starts with 169.254.xxx.xxx then see the next section.

If you have another IP address configured, then see section C.

B. I am getting an IP Address that starts with 169.254.xxx.xxx

If you are getting this IP Address, then you need to check that you are properly connected to the Router.

Confirm that you have a good link light on the Router for the port this computer is connected to. If not, please try another cable.

If you have a good link light, please open up a DOS window as described in the previous section and type ipconfig/renew.

If you are still unable to get an IP Address from the Router, reinstall your network adapter. Please refer to your adapter manual for information on how to do this.

C. My computer's IP Address is incorrect

If you have another IP address listed then the PC may not be configured for a DHCP connection. Once you have confirmed your computer is configured for DHCP, then please follow the steps below.

1. Open a DOS window as described above.
2. Type ipconfig/release.
3. Then type ipconfig/renew.

D. The 10/100 LED does not light after a connection is made.

1. Check that the host computer and the Router are both powered on.
2. Be sure the network cable is connected to both devices.
3. Verify that Category 5 cable is used if you are operating at 100 Mbps, and that the length of any cable does not exceed 100 m (328 ft).
4. Check the network card connections.
5. The 10BASE-T/100BASE-TX port, network card, or cable may be defective.

E. I can't get an Internet game, server, or application to work.

If you are having an issue getting any Internet server, application or game to function properly, you can expose the PC to the Internet using the DeMilitarized Zone (DMZ) function. This option is useful when an application requires too many ports or when you are not sure which ports to use. See section 7.8.6 to successfully configure this option

F. I am having problems establishing a PPPoE xDSL WAN connection

Some ISP's require you to enter the domain name in addition to your username and password. For instance, for SBC Global, enter username@sbcglobal.net. For Ameritech users, enter username@ameritech.net. BellSouth users may need to enter username@bellsouth.net and Mindspring subscribers enter username@mindspring.com. Lastly, Earthlink subscribers should enter either username@earthlink.net or ELN/username@earthlink.net.

G. Can I use this router with AOL DSL?

This is true in most scenarios. Please verify with AOL that your particular connection type is PPPoE. If yes, then the SMC VPN Broadband Router should work with your WAN connection. Follow the normal procedures as described in Section 7.3 of this manual, but while doing so, set the MTU value to 1400. AOL DSL does not allow for anything higher than 1400.

H. IPSec VPN Configuration

When setting up IPSec VPN tunnels between two BR14VPN, BR18VPN or one of each, it is imperative that you:

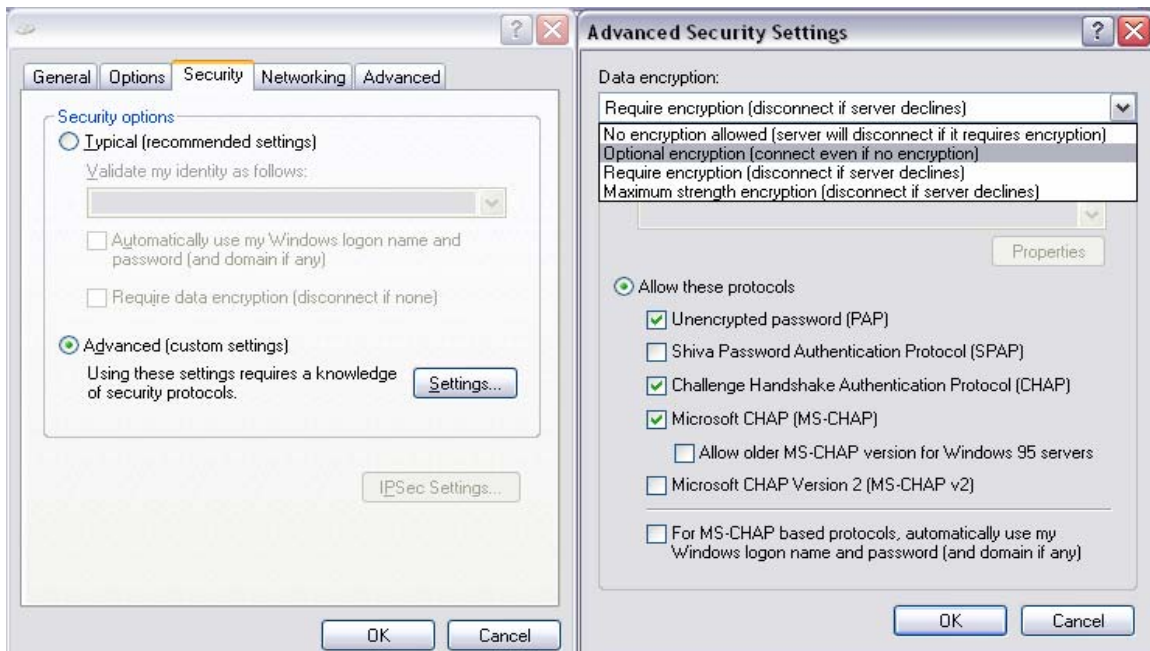
- a) Use the same pre-shared key between two endpoints
- b) Configuring matching IKE and IPSec proposals between two endpoints

To successfully create IPSec or IKE Proposal lists, you must configure the desired DH Group, Encryption/Authentication Algorithms, and Lifetimes, and then select the appropriate proposal ID and click the "Add to" button to add the proposal to the Index.

I. I have authentication problems with the L2TP or PPTP VPN Server

The Router's VPN Server will reject VPN clients that attempt to connect without the proper credentials. In the same token, if the VPN client is configured to connect only to encrypted networks, the client will not connect to the Router's VPN Server if it is configured for PAP or CHAP Authentication.

If you have configured the Router's VPN Server to use the PAP or CHAP Authentication Protocol, MPPE Encryption cannot be enabled. Therefore, you must configure the VPN client to connect the Router's VPN server without requiring encryption. By default, Windows VPN clients require encryption. You can go into the properties of the VPN connection and disable this requirement.



J. I forgot my password and can no longer log into the router.

You should restore your router to factory defaults via its hardware reset button. Locate the reset button (to the right of the power input). While the device is powered on, use a paper clip to depress this button for about 5-7 seconds and then release. Now you have completed the reset to factory defaults.

K. Upgrading the firmware

New firmware revisions will be made available as necessary when new product features or functionality is released. You should check <http://www.smc.com> on a periodic basis for these updates. If a new version is available, check the release notes to be sure of what has been changed/added and then you can decide if you wish to complete the upgrade. Then download and unzip the firmware file. Log into the web-based administration of the SMC Router, click TOOLS, then click FIRMWARE UPGRADE and browse to the new firmware file. Then click the "BEGIN UPGRADE" button to upload the firmware to the SMC Router. Once this is completed, be sure to reset the router to factory defaults and reconfigure your WAN connection before continuing to use it.

L. Why can't a PPTP client "see" the LAN clients on a SMCBR14VPN?

The PPTP and L2TP server IP address are different from the LAN IP. Therefore it could be possible for some OS, that PPTP clients can "see" each other but not the LAN clients. In order to solve this, one has to create a static route on the PPTP client.

For example:

```
route add 192.168.2.0 255.255.255.0 10.0.0.1
```

If 10.0.0.1 is your PPTP gateway and 192.168.2.1 is the remote LAN behind the router.

M. No IPSEC connect button?

There is no "Connect" button, the connection will be established on demand when a client from the peer is accessed.

The connection can be dropped with the "drop" button on the client list, but it will be re-established as soon as a client tries to access a remote peer.

N. L2TP won't work

Microsoft uses an embedded L2TP/IPSEC VPN implementation. In order to use the Microsoft standard VPN client, one has to disable the IPSEC on the PC. Please refer to Microsoft help to perform this operation.

9.1 | Questions and Answers

What is the difference between SMCBR14VPN and SMCBR18VPN?

The SMCBR14VPN has 4 LAN ports and the SMCBR18VPN HAS 8 LAN ports. There is no other difference. The firmware is the same for both.

How many tunnels can be configured?

40 IPSEC tunnels

5 PPTP tunnels

5 L2TP : Important, not L2TP/IPSEC, but just L2TP alone

In total: 50

Do I need two routers to establish a VPN connection?

No. PPTP tunnels and L2TP tunnels can be created with the built in Windows VPN tools

Although it is possible to use the built in IPSEC of Windows, it is much easier to use IPSEC client programs.

There are advantages when using 2 SMCBR14VPNs, especially when connecting two remote offices:

No configuration on end clients

End clients will just “see” the other office as if it was located on the same LAN.

Please remember that the two routers should have different LAN addresses.

Can the SMCBR14VPN act as a PPTP client?

No, it can only act as a PPTP and L2TP server

Can I use domain names and dynamic VPNs?

Yes. The SMCBR14VPN supports DynDNS on the WAN side.

As Peer IP address for the IPSEC tunnel, a domain name can be used

Dynamic VPN is supported, i.e. the router will accept a VPN connection from any IP address with valid parameters

10 | Technical Specifications

Standards:

IEEE 802.3 10Base-T Ethernet

IEEE 802.3u 100Base-TX Fast Ethernet

Hardware / Ports:

LAN Port	4x RJ45, 10/100 Mbps with Auto-MDI/MDIX (BR14VPN) 8x RJ45, 10/100 Mbps with Auto-MDI/MDIX (BR18VPN)
WAN Port	1x RJ45, 10/100 Mbps with Auto-MDI/MDIX
COM Port	1x DB9 (male), Up to 115200bps
Input Power	DC 5V2A

LEDs:

Power	1x Green LED for Power
WAN	1x Amber LED for 10Mbps link / Green LED for 100Mbps link Blinking LED when data is transmitted
LAN (4 port)	4x Amber LED for 10Mbps connection 4x Green LED for 100Mbps connection Blinking LED when data is transmitted
LAN (8 port)	8x Amber LED for 10Mbps connection 8x Green LED for 100Mbps connection Blinking LED when data is transmitted

VPN Pass-through:

IPSec

PPTP

LT2P

VPN Support:

IPSec Endpoint

PPTP Server

L2TP Server

Key management: IKE, Manual

Aggressive/Main mode for VPN

Remote gateway FQDN support

Dynamic VPN support

Encryption algorithm: DES, 3DES, AES

Authentication algorithm: MD5, SHA-1

PFS support

Keying Mode: Pre-Shared Key

Enabled NetBIOS Broadcast

Routing:

Static Route

Dynamic Route (RIP1/2)

WAN Connection Types:

Dial-Up

ISDN

PPPoE

Dynamic IP
L2TP
PPTP
BigPond
Static IP

Input Power:

5V 2A

Operating Temperature:

0~40°C

Humidity: 10%~90% non-condensing

Compliances:

FCC
CE
VCCI
UL

11 | Terminology

10BaseT - Physical Layer Specification for Twisted-Pair Ethernet using Unshielded Twisted Pair wire at 10Mbps. This is the most popular type of LAN cable used today because it is very cheap and easy to install. It uses RJ-45 connectors and has a cable length span of up to 100 meters. There are two versions, STP (Shielded Twisted Pair) which is more expensive and UTP (Unshielded Twisted Pair), the most popular cable. These cables come in 5 different categories. However, only 3 are normally used in LANs, Category 3, 4 and 5. CAT 3 TP (Twisted Pair) cable has a network data transfer rate of up to 10Mbps. CAT 4 TP cable has a network data transfer rate of up to 16Mbps. CAT 5 TP cable has a network data transfer rate of up to 100Mbps.

Access Point - A device that is able to receive wireless signals and transmit them to the wired network, and vice versa - thereby creating a connection between the wireless and wired networks.

Ad Hoc - An ad hoc wireless LAN is a group of computers, each with LAN adapters, connected as an independent wireless LAN.

Adapter - A device used to connect end-user nodes to the network; each contains an interface to a specific type of computer or system bus, e.g. EISA, ISA, PCI, PCMCIA, CardBus, etc.

Auto-Negotiation - A signaling method that allows each node to define its operational mode (e.g., 10/100 Mbps and half/full duplex) and to detect the operational mode of the adjacent node.

Backbone - The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Base Station - In mobile telecommunications, a base station is the central radio transmitter/receiver that maintains communications with the mobile radiotelephone sets within its range. In cellular and personal communications applications, each cell or micro-cell has its own base station; each base station in turn is interconnected with other cells' bases.

Bitmap - A Windows and OS/2 bitmapped graphics file format. Bitmap files provide formats for 2, 16, 256, or 16 million colors. It uses the extension .BMP.

BSS - BSS stands for "Basic Service Set". It is an Access Point and all the LAN PCs that are associated with it.

CHAP - When authenticating using Challenge Handshake Authentication Protocol (CHAP), the knowledge of the password, rather than the password itself is what is sent by the client. With CHAP, the VPN Broadband Router sends the remote client a challenge string. The remote client uses the challenge string and the password, and creates a Message Digest-5 (MD5) hash which is then forwarded to the VPN server. The VPN server computes the same hash calculation and compares the result with the hash sent by the client. If they match, the remote client is considered an authentic user.

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

DES - Data Encryption Standard. A cryptographic encryption algorithm that is part of many standards.

DHCP - Dynamic Host Configuration Protocol. This protocol automatically configures the TCP/IP settings of every computer on your home network.

DMZ - Allows a networked computer to be fully exposed to the Internet. This function is used when the special application sensing tunnel feature is insufficient to allow an application to function correctly.

DNS - DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as www.smc.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing " www.smc.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL - DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet - A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 million bits per second (Mbps).

ESS - ESS (ESS-ID, SSID) stands for "Extended Service Set". More than one BSS is configured to become an Extended Service Set. LAN mobile users can roam between different BSSs in an ESS (ESS-ID, SSID).

Fast Ethernet NIC - Network interface card that is in compliance with the IEEE 802.3u standard. This card functions at the media access control (MAC) layer, using carrier sense multiple access with collision detection (CSMA/CD).

Fixed IP - (see Static IP)

Full-Duplex - Transmitting and receiving data simultaneously. In pure digital networks, this is achieved with two pairs of wires. In analog networks, or digital networks using carriers, it is achieved by dividing the bandwidth of the line into two frequencies, one for sending, one for receiving.

Hub - Central connection device for shared media in a star topology. It may add nothing to the transmission (passive hub) or may contain electronics that regenerate signals to boost strength as well as monitor activity (active/intelligent hub). Hubs may be added to bus topologies; for example, a hub can turn an Ethernet network into a star topology to improve troubleshooting.

ID3 - The data fields in an MP3 that hold the artist name, track titles, album titles, genre, etc are known as ID3 tags.

IP Address - IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies an single, unique Internet computer host. Example: 192.34.45.8.

IP Security - Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

ISAKMP - Internet Security Association and Key Management Protocol. The basis for IKE.

ISP - Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

JPEG - Joint Photographic Experts Group. JPEG is a standard for compressing still images and it provides compression with ratios up to 100:1. File extensions are .JPG or .JPEG.

LAN - A communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link. Servers are high-speed machines that hold programs and data shared by network users. The workstations (clients) are the users' personal computers, which perform stand-alone processing and access the network servers as required.

Diskless and floppy-only workstations are sometimes used, which retrieve all software and data from the server. Increasingly, "thin client" network computers (NCs) and Windows terminals are also used. A printer can be attached locally to a workstation or to a server and be shared by network users. Small LANs can allow certain workstations to function as a server, allowing users access to data on another user's machine. These peer-to-peer networks are often simpler to install and manage, but dedicated servers provide better performance and can handle higher transaction volume. Multiple servers are used in large networks.

The message transfer is managed by a transport protocol such as TCP/IP and NetBEUI. The physical transmission of data is performed by the access method (Ethernet, Token Ring, etc.), which is implemented in the network adapters that are plugged into the machines. The actual communications path is the cable (twisted pair, coax, optical fiber) that interconnects each network adapter.

MAC Address - MAC (Media Access Control) A MAC address is the hardware address of a device connected to a network.

MDI / MDI-X - Medium Dependent Interface - Also called an "uplink port," it is a port on a network hub or switch used to connect to other hubs or switches without requiring a crossover cable. The MDI port does not cross the transmit and receive lines, which is done by the regular ports (MDI-X ports) that connect to end stations. The MDI port connects to the MDI-X port on the other device. There are typically one or two ports on a device that can be toggled between MDI (not crossed) and MDI-X (crossed).

Medium Dependent Interface - X (crossed) - A port on a network hub or switch that crosses the transmit lines coming in to the receive lines going out.

MP3 - MPEG Audio Layer 3. This is an audio compression technology that is included in the MPEG-1 and -2 specifications. MP3 encoding can allow you to compress CD-quality sound by a factor of 12.

MPEG - Moving Pictures Experts Group. MPEG is a standard for compressing video. MPEG-1 can provide resolution of 352x240 at 30 frames/second (fps) with 24-bit color and CD-quality sound. MPEG-2 can provide resolution of 704x480. MPEG uses the same intraframe coding as JPEG for individual frames, but also uses interframe coding which can help to further compress the video data, thereby reducing the overall size of the video.

NAT - (Network Address Translation) This process allows all of the computers on your home network to use one IP address. The NAT capability of the Barricade, allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP. Network Address Translation can be used to give multiple users access to the Internet with a single user account, or to map the local address for an IP server (such as Web or FTP) to a public address. This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network. NAT must be enabled to provide multi-user access to the Internet or to use the Virtual Server function.

Packet Binary Convulational Code(tm) (PBCC) - A modulation technique developed by Texas Instruments Inc. (TI) that offers data rates of up to 22Mbit/s and is fully backward compatible with existing 802.11b wireless networks.

PAP - This is a simple authentication protocol where the username and password data are both handled in a cleartext or unencrypted format. We do not recommend using PAP because your passwords are easily readable from the Point-to-Point Protocol (PPP) packets exchanged during the authentication process.

PCI - Peripheral Component Interconnect - Local bus for PCs from Intel that provides a high-speed data path between the CPU and up to 10 peripherals (video, disk, network, etc.). The PCI bus runs at 33MHz, supports 32-bit and 64-bit data paths, and bus mastering.

PPPoE - Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections. PPPoE is for Ethernet connections.

PPTP - PPTP stands for Point-to-Point Tunneling Protocol. It provides a means for tunneling IP traffic in Layer 2. For instance, it allows you to establish a connection to a corporate network and share files or other data as if your machine were actually on that local network.

Roaming - A function that allows your to move through a particular domain without losing network connectivity.

SNMP - Format used for network management data. Data is passed between SNMP agents (processes that monitor activity in hubs, switches, etc.) and the workstation used to oversee the network. SNMP uses Management Information Bases (MIBs), which are databases that define what information is obtainable from a networked device and what can be controlled (turned off, on, etc.).

Static IP - If your Service Provider has assigned a fixed IP address; enter the assigned IP address, subnet mask and the gateway address provided by your service provider.

SPI - Stateful Packet Inspection ensures that the data coming into your network was requested by an end node computer on your LAN. The Barricade examines the incoming data and compares it to a database of trusted information. As traffic leaves the network it is defined by certain characteristics. Incoming information is then compared to these sets of characteristics. If the incoming data matches the predefined set of characteristics the incoming traffic is allowed. If no match is found the incoming traffic is discarded.

Subnet Mask - A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet).

TCP/IP - Transmission Control Protocol/Internet Protocol. This is the standard protocol for data transmission over the Internet.

TCP - Transmission Control Protocol - TCP and UDP (User Datagram Protocol) are the two transport protocols in TCP/IP. TCP ensures that a message is sent accurately and in its entirety. However, for real-time voice and video, there is really no time or reason to correct errors, and UDP is used instead.

UDP - User Datagram Protocol - A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required. For example, UDP is used for real-time audio and video traffic where lost packets are simply ignored, because there is no time to retransmit. If UDP is used and a reliable delivery is required, packet sequence checking and error notification must be written into the applications.

VPN - Virtual Private Network that actually exists within a public network. This consists of a point-to-point tunnel through which users can send and receive data. The data packets are encrypted to provide for a true private connection to the endpoint (i.e. - corporate network). These packets cannot be decrypted without the correct encryption keys. Once the VPN tunnel is established, the client machine is authenticated and registered on the network. Given the proper privileges, it can then communicate directly with other machines as if it were actually on that local network.

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481
From Europe : Contact details can be found on
www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com

Driver updates:

http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:

<http://www.smc.com/>
<http://www.smc-europe.com/>

For Literature or Advertising Response, Call:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-91-352-00-40	Fax 34-93-477-3774
UK:	44 (0) 1932 866553	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 3355708602	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920	Fax 34 93 477 3774
Sub Saharan Africa:	216-712-36616	Fax 216-71751415
North West Africa:	34 93 477 4920	Fax 34 93 477 3774
CIS:	7 (095) 7893573	Fax 7 (095) 789 357
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-87978006	Fax 886-2-87976288
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-45-224-2332	Fax 81-45-224-2331
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

If you are looking for further contact information, please
visit www.smc.com or www.smc-europe.com.

Model number: SMCBR14VPN/ SMCBR18VPN

SMC
Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-
8000